Remarks

1) Claims 1-5, 12, 13, 15, 16, 17, 19, 21 are presented, of which claims 1, 12, 17 are independent, each of claims 2, 3-5 depends directly or indirectly on independent claim 1, claims 13, 15, 16 depends directly on independent claim 12, claims 19, 21 depends directly on independent claim 17.

2) Please note that the phrases used in the definition of identity software, that is, "with no protection against unauthorised use" in claim 1, third paragraph, line 2 and "with no individual and effective protection ...against unauthorised use" in claim 12, third paragraph, lines 1, 2 are being deleted because they are no longer necessary in the claims as amended and if the identity software as defined by claims 1, 12 as amended is protected against unauthorised use, the authorising software as defined by claims 1, 12 as amended can not discourage the user from enabling or allowing other person(s) to use the protected software or a duplication copy thereof, and this is required by the amended claims 1, 12, for which details will be discussed herein below.

3) In the Final Office Action, P.2, item 1c), claims 1-7 and 9-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Ananda(`645) .

In support of the rejections, the Examiner states, in the Final Office Action, P.2, item 3, that my arguments(response to First Office Action) filed on 18 Aug., 97 are not deemed to be persuasive for the reasons that a) "the rightful user make copies of ... software available" is probably the most prevalent form of unauthorised software distribution and b) "claim 12 specifies purchase and rental of software program is (as disclosed by Ananda) is merely a time-limited purchase".

The rejections are respectfully traversed.

The independent claims are being amended to better define the invention but without introducing any new issue. After the amendment, the independent

claims 1, 12, 17 claim an authorising software(claims 1 as amended) or protection software(claim 12 as amended) which comprises authorising software and identity software ; or authorising program(claim 17 as amended), stored in a device or existing physically on a medium, for use on a computer to protect other commercial computer software by discouraging a user thereof from enabling or allowing other person(s) to use the protected software or a duplication copy thereof.

The authorising software and identity software of claim 1 as amended, the protection software of claim 12 as amended, or authorising program of claim 17 as amended, conforming to or compatible with an existing standard so that they can be used on a computer (A) which also conforms to or compatible with that existing standard and without modification thereof.

The authorising software(claims 1, 12 as amended) or authorising program(claim 17 as amended) being for, when executed, authorising use of the protected software on computer (A).

The identity software(claims 1 or 2 as amended) or means for providing(claim 17 as amended) is for providing identity information of that user.

The identity information being for to be authenticated by a remote computer in order for enabling the remote computer to perform operation(s) for which that user has to be responsible.

Claim 1 as amended, claims the authorising software and, in particular, specifies that the authorising software also for determining the presence of an identity software on computer (A) and also that use of protected software on computer (A) will be authorised if the identity software is determined as being present on computer (A) .

Claim 12 as amended, claims a protection software comprising the authorising software and identity software and, in particular, specifies that they are contained in the protection software in such a manner that the authorising software is prevented from being copied therefrom individually ; and that the protected software is a

purchased software .

Claim 17 as amended, claims the authorising program and, in particular, specifies that information representative of an encryption algorithm used in the means for providing identity information, exists in the authorising program and being accessible or when the authorising program being executed, usable by the user thereof.

Thus, the present invention as defined by the amended claims is directed to using the presence of material X, which definition is readable on item **3A** herein below, as a precondition for authorising use of the protected software on a computer.

3A) Definition of "material X"

Please note that the identity software(claims 1, 12 as amended) or information representative of an encryption algorithm used in the means for providing identity information(claim 17 as amended) will be referred to as **"material X"** herein below and reasons therefor will be discussed in details in **item 3B** herein below.

3B) Whether "material X" is a useful material ?

Although material X is capable of being used for providing identity information of a user, for causing operation(s) for which that user has to be responsible, it is actually being used as a material by the present invention as defined by the amended claims, for affecting human behaviour.

Specifically, as the identity information of a user is for causing operation(s) the user has to be responsible for, and a user in general will not copy or provide his/her identity software(claims 1, 12) or means for providing his/her identity information(claim 17) , i.e., material X, to someone else, in order to protect himself/herself from having to take the responsibility of operation(s) caused by that someone else, even though the user may do this provided that both of them have a good enough relationship for him/she to do so. Therefore, material X is capable of

affecting human being behaviour in such a way that it is capable of being used as a **psychological barrier** to prevent that user from copying or providing itself or other material inseparable therefrom, to someone else.

Material X is thus analogous to the bait used in a mouse trap, and one example of such a mouse trap is readable on a patent invention entitled "Jar Lid Mouse Trap" issued to La Rue, Date Nov., 23, 1976, patent # : 3,992,802, inwhich a mouse trap for trapping a mouse within a jar is disclosed, and as readable on the abstract, the mouse trap has a bait holder to hold a bait for to be taken by a mouse. As seen, the bait is a material capable of affecting animal behaviour in such a way that it attracts a mouse to get into a mouse trap.

Although the bait is not the patentable subject matter, the issuing of La Rue's patent does show that the Patent and Trademark Office has accepted that the bait is **useful**, and its usefulness make the mouse trap a **useful** device and can thus be patented.

Similarly, material X should also be **useful** because affecting human behaviour(material X) and affecting animal behaviour(material bait) is an immaterial variation.

Further, for many instances, **the Patent and Trademark Office** has shown that it **accepts** inventions which make use of **psychological barrier**, rather than physical barrier, to prevent unauthorised or illegal activities, as useful and can be patented. For one instance, patent # : 5,437,323, entitled : Burglar deterrent decoy, it is disclosed in the abstract that, a decoy consists of a partial face mask with simulated eyes and nose ..mounted...behind a window blind...to produce an illusion that a person is looking out through the window blind to scare away a burglar. For another instance, patent # : 5.358,025, entitled : Fabric garage enclosure, it is disclosed in the abstract that, an enclosure device which can be utilised to cover a garage door opening for privacy and security. The device includes a fabric portion(which being non-rigid, as readable on claim 1) which acts as a psychological barrier to possible intruders who

would be unable to determine if the garage is occupied.

3C) Whether the present invention as defined by independent claims 1, 12, 17, anticipated by Ananda ?

The present invention as defined by the amended claims, **is directed to making use of the above-mentioned capability of affecting human behaviour** of material X, **to protect other software**, namely as, the authorising software(claim 12 as amended) or authorising program(claim 17 as amended) and the protected software(claims 1, 12, 17 as amended), **by using the presence of material X on a computer as a precondition for authorising use of protected software on that computer**, and thereby, discouraging a user from enabling or allowing other person(s) to use the protected software or a duplication copy thereof, and this is neither disclosed or suggested or described by Ananda's claims.

It is respectfully submitted that, software is capable of being copied, and it is therefore **an important innovative feature** of the present invention as defined by the amended claims 1, 12, 17 that to protect software, i.e., authorising software(claim 12 as amended) or authorising program(claim 17 as amended) or protected software(claims 1, 12, 17 as amended) against piracy copying, by means of another software, i.e., the identity software(claims 1, 12) or information representative of an encryption algorithm used in the means for providing identity information(claim 17 as amended), which being contained in a software program, i.e., the authorising program(claim 17 as amended).

Ananda, as readable on all the claims thereof, describes a method of securely renting software, and as readable on claim 1, merely teaches of permitting continuous execution of application software in a first computer if authorisation is obtained from a second computer continuously, and execution will be terminated if otherwise. Claim 11 claims a similar method and in particular, specifies a rental application comprising a header program for, when being executed, transmitting from the first computer a

password verification request comprising a system time, to the second computer, and the second computer will return a dynamic password in response, and the header program terminates the rental application if the dynamic password received does not match another dynamic password it generated using that system time previously. And, the purpose of the invention is readable on col. 23, lines 44-53, "The invention enables ... monitor the time period when a particular application software is executed by a user .... record the pertinent information regarding the execution of application software .... for billing and accounting purpose".

There is no software/means in Ananda's claimed invention which can meet the requirement of identity software of claims 1, 12(before and after this amendment) or means for providing identity information of claim 17(before and after this amendment). Ananda's claims merely mention of a password verification request comprising a system time and there has no description in Ananda's claims as to whether user's identity has to be authenticated and if it has to be, in what way this should be done.

Accordingly, withdrawal of the rejections of independent claims 1, 12, 17 and their dependent claims 2, 3-5, 13, 15, 16, 19, 21 under 35 U.S.C. 102(e) as being anticipated by Ananda(`645) are respectfully requested.

4) In the final office action, item 2a, claims 1, 2, 3-5, 12, 13, 15, 16, 17, 19, 21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Examiner states that, "The claims are full of grammatical errors and dangling clauses which make the scope of the claims, indeterminate."

The rejections are respectfully traversed. The independent claims and dependent claims are being amended to eliminate grammatical errors and dangling clauses therein, so as to make the scope of the claims determinable.

Accordingly, withdrawal of the rejections of claims 1, 2, 3-5, 12, 13, 15, 16, 17, 19, 21 under 35 U.S.C. 112, second paragraph, are respectfully requested.

5) In the final office action, item 2b, claims 1, 2, 3-5, 12, 13, 15, 16, 17, 19, 21 are rejected as failing to define the invention in the manner required by 35 U.S.C. 112, second paragraph.

The Examiner states that "the claims replete with indefinite and functional or operational language" and also that "the structure which goes to make up the device must be clearly and positively specified" and further that " The structure must be organised and correlated in such a manner as to present a complete operative device" and further that "For examination purpose, the claimed invention is understood as a software method".

The rejections are respectfully traversed. The Examiner incorrectly interprets the invention as defined by independent claims 12, 17 as a computer base device.

As mentioned herein above in item **3B** that, the identity software(claims 1, 12 as amended) or information representative of an encryption algorithm(claim 17 as amended) is a **useful material** capable of affecting human being behaviour in such a way that it make that user tends to protect it from being used by someone else.

Claim 1 as amended present an authorising software onwhich a software method comprising the steps of 1) determining the presence of material X on a computer, 2) authorising use of the protected software if material X is determined as being present ; is readable.

Claims 12, 17 as amended **present protection software**(claim 12 as amended) **or authorising program**(claim 17 as amended) **which is also a useful material** because it includes a useful material X therein, and has a well-defined composition.

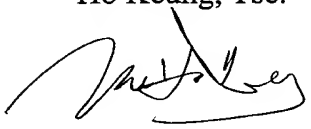
Thus, the requirement of 35 U.S.C. 112, second paragraph is being met by claims 1, 12, 17 as amended.

Accordingly, withdrawal of the rejections of claims 1, 2, 3-5, 12, 13, 15, 16, 17, 19, 21 as amended under 35 U.S.C. 112, second paragraph, are respectfully requested.

Date: March., 16, 98

Respectfully submitted,

Ho Keung, Tse.



Software for restricting other software to be used by the rightful user only

Field of the invention

The present invention relates to protection of commercial software supplied through a communication link or the like, and particularly, to protection of such software against unauthorised use.

Background of the invention

Conventionally, software protection methods for protecting commercial software products such as programs, multimedia software, supplied through a communication link, such as a telephone line, require a user computer to have a piece of hardware which comprises, for instance, decryption keys and system be installed therein for to be authenticated by a software program running on the computer. Hardware, rather than software, are being used because software duplication facilities are commonly found in personal computers. However, this is extremely cumbersome and places a large burden on users and vendors alike.

It is therefore an object of the present invention to provide a piece of software to replace the above-mentioned piece of hardware and its rightful user is being discouraged from copying it to someone else.

It is therefore another object of the present invention to provide a method to discourage a rightful user of commercial software from copying the commercial software to someone else.

Summary of the invention

According to a first embodiment of the present invention, there is provided a central program comprising 1) a sub-program for providing an Encrypted Identity (hereinbelow referred to as EI sub-program), 2) a sub-program for

authorising use of a software product (hereinbelow referred to as ES sub-program), 3) a sub-program for authenticating user computer (hereinbelow referred to as AC sub-program).

The central program is for managing the use of the individual sub-programs therein so that the ES sub-program can be protected from being accessed by the user directly, thereby preventing it from being copied individually. The EI sub-program is for providing an encrypted identity of a user for accessing a network central computer to obtain services or software products or alike inwhich a secure operation on a user account for payment therefor involved. The AC sub-program is for authenticating the computer on which it runs by determining the hardware and software configuration as well as hardware characteristics of the computer by software means and comparing the result with that required. The ES sub-program is for using the authentication result of the AC sub-program and the presence of the EI sub-program as preconditions for authorising those software products obtained to be used on a computer.

← readable on the corresponding part of the original spec.

It should be noted that in the central program, as far as protection of the software products from being unlawfully copied by the rightful user to someone else is concerned, the ES sub-program is the one which needs protection and according to the present invention, the ES sub-program is protected from being unauthorised copied by its rightful user to someone else lies on the fact that a rightful user would not copy a program, i.e., the EI sub-program, which can provide the rightful user's encrypted identity for using the rightful user's account in obtaining, for eg., network services or software products, to someone else. As seen from the use of automatic teller machine(ATM) magnetic cards, which although can readily be forged, has been proved to be remarkably secure.

According to a second embodiment of the present invention, the central program comprising the EI sub-program only, and the ES sub-program authorises the software product(s) to be used only when the EI sub-program is present on the same computer and which is being determined by receiving an encrypted identity of the EI

sub-program from the same.

According to a third embodiment, the EI and ES sub-programs are basically equivalent such that copying the ES sub-program by its rightful user to someone else is equivalent to copying the EI sub-program to someone else, thereby preventing the ES sub-program from unauthorised copied or use.

Brief description of drawings

FIG.1 is a block diagram of the central program.

FIG.2 is a diagrammatic view of a program inwhich a part B thereof being encrypted, in RAM space.

Detailed description of the preferred embodiments

The present invention is directed to protecting software product(s) supplied through a communication link, and for the sake of simplicity, the following description is directed to protection of such software product(s) stored in a user's IBM PC computer, against unauthorised copying or use. And, the present invention will be described under the following headings:

1) The Central Program.

2) The Sub-program for providing an Encrypted Identity (EI sub-program).

3) The Sub-program for authorising use of a software product (ES sub-program).

4) The Sub-program for authenticating user computer (AC sub-program).

5) Other Embodiments.

1) The Central Program.

According to the first embodiment, there is provided a central program which being an executable program and can be caused to be executed a) by user by entering its filename in DOS environment, b) by a running program. FIG.1 is a block diagram of the central program.

a) If a user desires to access a network central computer through a communication link, the user has to cause the central program to be executed.

Then the central program will cause the EI sub-program, of which details will be described herein below, to be executed for providing an encrypted identity of the user, to the central computer. The central computer will permit the access request from the user if the encrypted identity is correct, for which details will be described in item 2 herein below.

b) When a running program desires to cause the ES sub-program to be executed, to authorise it to continue to run, it will first prepare an input parameter for indicating to the central program such a request and store the input parameter in a predetermined location in RAM, then through the use of a PC DOS service call for that purpose, cause the central program to be executed. The central program will first access the input parameter in the predetermined location and from it the central program can determine that a running program is requesting for an authorisation command from the ES sub-program, and will then cause the ES sub-program to be executed.

For the case the central program is being caused by user to be executed, there will be no valid or no input parameter and the central program can thus know this fact.

2) The Sub-program for providing an Encrypted Identity (EI sub-program).

This sub-program borrows the technique used in IC credit card for identity authentication inwhich an encrypted identity is generated.

When starts, the EI sub-program sends an access request to the central computer which in return will send back a random number. The EI sub-program will then encrypt the random number with a predetermined algorithm A1 and send the result to the central computer which will permit access if the result is identical with another result it obtained by performing the same encryption algorithm on that random number.

It should be noted that for each user, there is a corresponding respective encryption algorithm A1 for the identification thereof and also that the central computer may use the encryption result from the EI sub-program, if it being correct, as a user authorisation for payment to be made, from a user account for obtaining network services or software products or the like.

3) The Sub-program for authorising use of a software product (ES sub-program).

According to the present invention, there are 2 approaches for authorising use of a software product :

i) by sending encrypted commands to a running software program for authorising continuous use of the same on a computer, by the technique as mentioned above in item 2 for identity authentication. Specifically, the running software program includes in the input parameter, as mentioned above in item 1b, a random number it generated, then causes the central program to be executed. The ES sub-program, which being caused to be executed by the central program, as mentioned above in item 1b, sends the result it obtained by performing a predetermined encryption algorithm A2 on that random number, to the running software program which will compare the result with another result it obtained by performing the same encryption algorithm A2 on that random number.

It should be noted that for each user, each of the software products for use on his/her computer(s) use a same respective encryption algorithm A2 and the encryption algorithm A2 being included into each such software product by the central computer at the time when the central computer is to supply the same to the user computer.

ii) by decrypting an encrypted part of a software product or an encrypted software product.

It should be noted that if the software product is a program, then it will be sufficient to have a part thereof to be encrypted, for preventing unauthorised copying and use, however, if the software product is an audio/visual multimedia data file, it should be more desirable to have the whole software product be encrypted.

The decryption of a part of or an entire software product takes place on a temporary copy of which in RAM. Given by example only, FIG. 2 is a diagrammatic view of a program in RAM space, with a part B thereof being encrypted. As seen, the ES sub-program decrypts part B and stores the result which size should be not equivalent to that of the encrypted copy, in 'part B decrypted'.

The ES sub-program then overwrites at the first location of 'part B encrypted' an instruction 'JUMP TO part B decrypted' and at the end of 'part B decrypted' appends an instruction 'JUMP TO part C'. In this way, the encrypted part of the software will not be executed and the decrypted part will be executed instead.

In the case of audio/visual multimedia software, the software will be decrypted a small part by a small part and each small part is decrypted at the time it is about to be utilized by a audio/visual program for causing audio/visual effect. In other words, that audio/visual program has to cause the ES sub-program to be executed in the manner as described above in item 1b, everytime it wants a decryption of a small part. Desirably, a newly decrypted small part will overwrite a previously decrypted one so that a whole copy of the decrypted software will not exist in RAM.

4) The Sub-program for authenticating user computer (AC sub-program).

One object of this sub-program is to prevent the central program from being used , if it being a copy made by someone other than the rightful user and of this the rightful user being unaware, so that a rightful user need not guard his computer containing the central program from reach of someone else.

When the central program is being installed in a harddisk of a user computer and executed, it will check an encrypted status information stored in itself and from which it knows this is the first time it being executed and will cause an initialization process to take place. In the initialization process, the central program sends to the central computer, as mentioned herein above in item 2, an unencrypted identity of the user, then the AC sub-program requests for an encrypted command from the central computer which will provide such an encrypted command, in the manner as described hereinabove in item 3i, if the user has a valid account or the account is not closed.

After authenticating the command, the AC sub-program determines the hardware and software configuration of the user computer, which includes, for eg., running speed determination which is a function of CPU frequency, cache memory size etc; number and identities of peripherals such as mouse, printer, joystick, harddisk and floppy disk drive etc; characteristics of hardware such as number of heads, cylinders, sectors of harddisk and locations of bad sectors therein; version number of operation system software and physical position of a particular software product including the central program in the harddisk; by skills well known to those in the art. For instance, the running speed can be determined by causing the computer to execute a test program and initializing a hardware counter to measure the time the computer has taken to finish executing the program. For another instance, the version number of the operation system may be determined by using a particular DOS service call.

The result of the determination and a status information indicative of the central program being initialized is being stored by the AC sub-program in a predetermined part of the central program in the harddisk, in the form of encrypted data. Thereafter, everytime when the central program is executed, it will first check the status information, and after determining that it is being initialized, it will perform a job as requested, as mentioned in item 1 herein above, and in addition thereto, it will also automatically cause the AC sub-program to be executed which will determine at

least a part of the above-mentioned hardware and software configuration as well as hardware characteristics of the computer, at a time, and the AC sub-program will encrypt an indication information in another predetermined part of the central program for causing the ES sub-program not to operate, if any part of the configuration/characteristics determined is not identical to the corresponding part of that it encrypted and stored previously.

In addition thereto, the AC sub-program will also reset the encrypted status information so that another initialization process will automatically take place when the user causes the central program to be executed, and for the authorisation of which another encrypted command from the central computer will be required.

This also prevents a user from deliberately adapting the central program to computer of other user(s), after closing his account.

In addition, the encrypted command from the central computer may alternatively be supplied to the user via, eg., a telephone line, and then entered into the user computer by the user. Specifically, to request for an encrypted command, the AC sub-program generates a random number and conveys the random number to the user who in turn supplies it to the central computer by means of telephone dual tone signals, generated by entering the random number on a telephone keypad, through the telephone line, and after encrypting the random number, the central computer sends the result to the user via the same telephone line by means of a voice synthesizer.

5) Other Embodiments

According to the second embodiment, the ES sub-program is separated from the central program and become an independent program, whereas the central program [which] comprises the EI sub-program only. The ES program is bound to the EI sub-program by requiring the ES program to operate only when the EI sub-program is present on the same computer. Specifically, the ES program when running, can cause the EI sub-program to be executed for generating an encrypted identity for

the ES program to authenticate. The EI sub-program knows that this is a request for encrypted identity from the ES program, not a request from user for encrypted identity for accessing the central computer, by the technique of input parameter as mentioned above in item 1b.

Further, the EI sub-program before sending the encrypted identity to the ES program, may first check the data integrity of itself by, for instance, checksum method. Alternatively, it may also be that the ES program performs the checking. And, if the checking result is that some data in the EI sub-program being altered, then in the former case, the ES will be caused to be not operable by the EI sub-program by not sending it an encrypted identity, and in the latter case, the ES program will be caused to be not operable by itself.

According to the third embodiment, the encryption algorithms A1 and A2 that the EI and ES sub-programs use respectively for providing an encrypted identity to the central computer and for generating encrypted commands to authorise use of a software product respectively, is a same algorithm.

Thus, it would be equivalent for a rightful user to copy his EI sub-program to someone else if he copies his ES sub-program to someone else. In this case, a slight modification on the ES sub-program can make it equivalent to the EI sub-program and which involves adding a simple interface program for receiving a random number from the central computer, feeding the random number into the ES sub-program, receiving the encryption result from the ES sub-program and supplying the encryption result to the central computer, and such functions are commonly found in any network interface software.

In addition, according to another embodiment of the present invention, the software products and ES sub-program each includes an identity of its rightful user, so as to facilitate legal action against piracy. Further, the ES sub-program, when executed, will access each of the software products, by using a particular DOS service call for loading a software product stored in the computer onwhich it runs, from

harddisk to RAM, for checking such an identity therein, if any software product is found to have an identity not identical to that of the ES sub-program, the ES sub-program will inhibit use of all software products under its control, including itself, on the computer. Such identities may be stored in a predetermined location of the software products, and is protected from being altered by having an encrypted one stored in another location in each software product, and each of those another locations is different in different software products so that it would not be discovered and altered. And, each such software product, when executed, will automatically check the unencrypted identity stored therein against the decryption result of the encrypted one, if they are not consistent, the software product will fail to operate. The identity or encrypted identity of the rightful user being included into each of the software products by the central computer at the time when the central computer is to supply the same to the user computer. Further, to prevent the ES sub-program from mistakenly regarding a software product which stored in the computer and which being not supplied from the central computer, as a software product under its control, the central computer may further include information in another predetermined location of each software product for indicating this fact, that is, the software product being supplied from the central computer, to the ES sub-program and each software product will not operate if when being executed, it finds that information therein being altered.